Declassified in Part - Sanitized Copy Approved for Release 2011/11/04 : CIA-RDP95B00890R000700190045-5

General Services Administration
Information Security Oversight Office
Washington, DC 20405

September 13, 1983

DD/A Registry
83-0932/1

Mr. Harry E. Fitzwater
Deputy Director for Administration
Central Intelligence Agency
Washington, DC 20505

Dear Mr. Fitzwater:

Executive Order 12356, "National Security Information," has been in effect for over a year now. Under the Order, the Information Security Oversight Office (ISOO) continues to monitor the government-wide information security program.

While much will depend upon an upcoming analysis of relevant statistical data, ISOO's preliminary findings are that, on balance, it has been a very successful year. We list the perceived strengths and weaknesses of the past year's effort in an enclosure to this letter. This enclosure also addresses some other subjects of interest.

We also enclose a copy of the new Standard Form 189, "Classified Information Nondisclosure Agreement," and a copy of the final rule that implements its usage. Agencies will use the SF 189 to fulfill the requirements of paragraph 1(a) of National Security Decision Directive 84 (NSDD-84), entitled "Safeguarding National Security Information," that the President issued on March 11, 1983. The Director of Central Intelligence is issuing the Sensitive Compartmented Information Nondisclosure Agreement mandated by paragraph 1(b) of NSDD-84. ISOO liaisons will be contacting their agency counterparts in the next week or so to arrange deliveries of initial stocks of the SF 189. You will be responsible for procuring subsequent orders through regular channels. You must retain the completed forms in a file system that will assure their expeditious recovery for the 50 year retention period that ISOO is recommending to the Archivist of the United States under the Records Disposal Act. (This retention period corresponds to the presumed period of continuing national security sensitivity for certain intelligence and cryptological information.) If you have any questions concerning the use of the SF 189 that are not addressed in the final rule, please contact me or your ISOO liaison as quickly as possible.

You and your staff, as the senior officials responsible for the information security program, deserve much of the credit for the smooth transition under E.O. 12356. We urge you to continue your commitment to achieving the critically important objective of managing our legitimate security needs within the framework of open government.

Sincerely,

STEVEN GARFINKEL
Director

Enclosures

OS REGISTRY
0249/10-83

OBSERVATIONS AND REMINDERS

I. General Observations about the Pluses and Minuses for the First Year of Executive Order 12356

A. Pluses

1. The transition from E.O. 12065 to E.O. 12356 went very smoothly. ISOO attributes this to two factors: the involvement and commitment of program officials within the critical agencies, and the relative similarity between the two information security systems in ordinary operations.

2. No legitimate "horror stories" have arisen to undermine the revised information security system. Despite unparalleled scrutiny, program managers have avoided the serious classification abuses predicted by E.O. 12356's critics.

3. The positive impact of E.O. 12356's revisions is slowly but surely being realized. Program managers have more flexibility in their administration of the information security system. The burden of litigating the "balancing test" is abating. Our allies are expressing greater confidence in our ability to protect shared information.

B. Minuses

1. There has been some indifference among persons at the operating level about the revised information security system. ISOO attributes this largely to an understandable sense of frustration at the prospect of a fourth operable Executive order on national security information within a decade.

2. Despite an unprecedented effort to "get the word out" to operating personnel about E.O. 12356, too many persons who work with classified information remain unfamiliar with its requirements. Inaccurate media accounts of the Order and the indifference mentioned above aggravate this situation.

3. Too many documents are not being portion marked even though they are transmitted outside the originating office and are used as sources for derivative classification. In addition, too many documents that are clearly sensitive for a determinable period of time are being marked "OADR."

II. Reporting Unauthorized Disclosures to ISOO

Both E.O. 12356 and National Security Decision Directive 84 require that agencies report instances of unauthorized disclosures of classified information to ISOO. To date, there has been haphazard compliance with this reporting requirement.

ISOO does not investigate "leaks," nor should it interfere in such investigations. Its role is limited to determining if the unauthorized disclosure resulted from a problem with the information security system itself, rather than an instance of a person willfully deviating from prescribed standards.

Each agency should report to ISOO any unauthorized disclosure that appears to involve a systemic problem as soon as the agency has completed its preliminary inquiry. Each agency should ordinarily report any other unauthorized disclosure to ISOO if and when the agency refers the matter to the Department of Justice. However, an agency and ISOO may establish alternative procedures for reporting unauthorized disclosures when such arrangements enhance the protection of classified information. Please contact the ISOO Director or your ISOO liaison if your agency wants to establish alternative procedures for reporting unauthorized disclosures.

III. Statistical Reports Due by October 31, 1983

Each agency's Standard Form 311, "Agency Information Security Program Data," for the reporting period August 1, 1982 through September 30, 1983, is due at ISOO no later than October 31, 1983. It is very important that you file your reports on time this year because of the great interest in the data that reflect the first 14 months of E.O. 12356.

IV. Training Aids

ISOO's award-winning slide/tape or videocassette briefing on E.O. 12356 is available now from the National Audiovisual Center and will shortly be available from the Defense Audiovisual Agency. Please contact your ISOO liaison for further information.

ISOO still has some copies of its booklet on Marking National Security Information. In addition, ISOO is having another printing made of its FY 82 Report to the President, which includes an essay on "The Background of Executive Order 12356." This essay is intended to clear up a number of misconceptions about the purposes behind the issuance of the new Order. These are available upon request to your ISOO liaison.

CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

An Agreement Between _____ and the United States
(Name - Printed or Typed)

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. As used in this Agreement, classified information is information that is either classified or classifiable under the standards of Executive Order 12356, or under any other Executive order or statute that prohibits the unauthorized disclosure of information in the interest of national security. I understand and accept that by being granted access to classified information, special confidence and trust shall be placed in me by the United States Government.

2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of classified information, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures.

3. I have been advised and am aware that direct or indirect unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge such information unless I have officially verified that the recipient has been properly authorized by the United States Government to receive it or I have been given prior written notice of authorization from the United States Government Department or Agency (hereinafter Department or Agency) last granting me a security clearance that such disclosure is permitted. I further understand that I am obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information.

4. I have been advised and am aware that any breach of this Agreement may result in the termination of any security clearances I hold; removal from any position of special confidence and trust requiring such clearances; and the termination of my employment or other relationships with the Departments or Agencies that granted my security clearance or clearances. In addition, I have been advised and am aware that any unauthorized disclosure of classified information by me may constitute a violation or violations of United States criminal laws, including the provisions of Sections 641, 793, 794, 798, and 952, Title 18, United States Code, the provisions of Section 783(b), Title 50, United States Code, and the provisions of the Intelligence Identities Protection Act of 1982. I recognize that nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.

5. I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result or may result from any disclosure, publication, or revelation not consistent with the terms of this Agreement.

6. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement.

7. I understand that all information to which I may obtain access by signing this Agreement is now and will forever remain the property of the United States Government. I do not now, nor will I ever, possess any right, interest, title, or claim whatsoever to such information. I agree that I shall return all materials which have, or may have, come into my possession or for which I am responsible because of such access, upon demand by an authorized representative of the United States Government or upon the conclusion of my employment or other relationship with the Department or Agency that last granted me a security clearance. If I do not return such materials upon request, I understand that this may be a violation of Section 793, Title 18, United States Code, a United States criminal law.

8. Unless and until I am released in writing by an authorized representative of the United States Government, I understand that all conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to classified information, and at all times thereafter.

9. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect.

10. I have read this Agreement carefully and my questions, if any, have been answered to my satisfaction. I acknowledge that the briefing officer has made available to me Sections 641, 793, 794, 798, and 952 of Title 18, United States Code, Section 783(b) of Title 50, United States Code, the Intelligence Identities Protection Act of 1982, and Executive Order 12356, so that I may read them at this time, if I so choose.

11. I make this Agreement without mental reservation or purpose of evasion.

SIGNATURE	DATE	SOCIAL SECURITY NO. *(See notice below)*

ORGANIZATION

The execution of this Agreement was witnessed by the undersigned, who, on behalf of the United States Government, agreed to its terms and accepted it as a prior condition of authorizing access to classified information.

WITNESS AND ACCEPTANCE:

SIGNATURE	DATE

ORGANIZATION

NOTICE: The Privacy Act, 5 U.S.C. 552a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Account Number (SSN) is Executive Order 9397. Your SSN will be used to identify you precisely when it is necessary to 1) certify that you have access to the information indicated above or 2) determine that your access to the information indicated has terminated. Although disclosure of your SSN is not mandatory, your failure to do so may impede the processing of such certifications or determinations.

STANDARD FORM 189 (8-83)
Prescribed by GSA/ISOO
32CFR 2003; E.O. 12356

Federal Register

Friday
September 9, 1983

Part III

Information Security Oversight Office

National Security Information; Standard Forms; Final Rule

INFORMATION SECURITY OVERSIGHT OFFICE

32 CFR Part 2003

National Security Information; Standard Forms

AGENCY: Information Security Oversight Office (ISOO).

ACTION: Final rule.

SUMMARY: This rule provides for the use within the executive branch of standard forms that pertain to national security information. These forms are issued in accordance with the provisions of Section 5.2(b)(7) of Executive Order 12356.

EFFECTIVE DATE: September 9, 1983.

FOR FURTHER INFORMATION CONTACT: Steven Garfinkel, Director, ISOO. Telephone: 202-535-7251.

SUPPLEMENTARY INFORMATION: Section 5.2(b)(7) of Executive Order 12356 authorizes the Director of ISOO to prescribe the use of standard forms that will promote the implementation of the government-wide information security program. ISOO has developed these forms in coordination with those agencies that will be primarily affected by them.

List of Subjects in 32 CFR Part 2003

Classified information, Executive orders, Information, National security information, Security information.

Title 32 of the Code of Federal Regulations, Chapter XX, is amended by adding a new Part 2003 to read as follows:

PART 2003—NATIONAL SECURITY INFORMATION—STANDARD FORMS

Subpart A—General Provisions

Sec.

Subpart B—Prescribed Forms

Authority: Sec. 5.2(b)(7) of E.O. 12356.

Subpart A—General Provisions

§ 2003.1 Purpose.

The purpose of the standard forms prescribed in Subpart B is to promote the implementation of the government-wide information security program. Standard forms are prescribed when their use will enhance the protection of national security information and/or will reduce the costs associated with its protection.

§ 2003.2 Scope.

The use of the standard forms prescribed in Subpart B is mandatory for all departments, and independent agencies or offices of the executive branch that create and/or handle national security information. As appropriate, these departments, and independent agencies or offices may mandate the use of these forms by their contractors, licensees or grantees who are authorized access to national security information.

§ 2003.3 Waivers.

Except as specifically provided, waivers from the mandatory use of the standard forms prescribed in Subpart B may be granted only by the Director of ISOO. The Director of ISOO will be responsible for ensuring that all waivers that necessitate changes to a standard form are cleared with the General Services Administration's Office of Information Resources Management (KLSO) as an exception to the standard form (41 CFR 101-11.8).

§ 2003.4 Availability.

Agencies may obtain copies of the standard forms prescribed in Subpart B by ordering through FEDSTRIP/MILSTRIP or by including the required quantities on a Standard Form 3146 signed by an agency approving official for self-service store purchases. The national stock number of each form is cited with its description in Subpart B.

Subpart B—Prescribed Forms

§ 2003.20 Classified Information Nondisclosure Agreement: SF 189.

(a) SF 189 is a nondisclosure agreement between the United States and an individual that is to be executed as a condition prior to the United States Government authorizing that individual access to classified information.

(b) All employees of executive branch departments, and independent agencies or offices, and the employees of their contractors, grantees and licensees must sign SF 189 as a condition prior to being authorized access to classified information. This requirement may be implemented prospectively by an agency for which the administrative burden of compliance would be excessive. Only the National Security Council may grant an agency's application for prospective implementation. To request prospective implementation, an agency must submit its justification to the Director of ISOO, who will forward it with a recommendation to the National Security Council.

(c) Agencies may require other persons, who are not included under paragraph (b), above, to execute SF 189 as a condition prior to receiving access to classified information.

(d) Only the National Security Council may grant an agency's application for a waiver from the use of SF 189. To apply for a waiver, an agency must submit its proposed alternative nondisclosure agreement to the Director of ISOO, along with its justification. The Director of ISOO will request a determination about the alternative agreement's enforceability from the Department of Justice prior to making a recommendation to the National Security Council.

(e) Each agency must retain its executed copies of the SF 189 in file systems from which the agreements can be expeditiously retrieved in the event that the United States must seek their enforcement.

(f) The national stock number for the SF 189 is 7540-01-161-1869.

Dated: September 6, 1983.

Steven Garfinkel,

Director, Information Security Oversight Office.

[FR Doc. 83-24688 Filed 9-8-83; 8:45 am]

BILLING CODE 6820-AF-M